IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN RE ENZO BIOCHEM DATA BREACH LITIGATION	**Lead Case No. 2:23-cv-04282-GRB-AYS**
	CONSOLIDATED CLASS ACTION COMPLAINT
This Document Relates To: All Cases	**JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Elyssa Crimeni, Elizabeth Delgrosso, Annette DiIorio, Eliana Epstein, Elizabeth Garfield, Gita Garfinkel, Mark Guthart, Tony Johnson, Nino Khakhiashvili, Margo Kupinska, Paula Magnani, Shana McHugh, Mary Namorato, Robert Pastore, Saribel Rodriguez, and Izza Shah bring this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Enzo Biochem, Inc. ("Enzo Biochem") and Enzo Clinical Labs, Inc. ("Enzo Clinical," and collectively with Enzo Biochem, "Enzo" or "Defendants") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs.

NATURE OF CASE

1. This class action arises out of the recent, targeted cyberattack and data breach where third-party criminals retrieved and exfiltrated personal data from Enzo's network resulting in unauthorized access to the highly sensitive consumer data of Plaintiffs, and, according to Enzo,

at least 2,470,000 Class Members ("Data Breach").[1] After learning of the Data Breach, Enzo Defendants waited nearly two months to notify affected individuals.

2. Enzo Biochem is a leading life sciences and biotechnology company, based in New York. [2] Enzo Clinical, a wholly-owned subsidiary of Enzo Biochem, is a New York-regional full service clinical reference laboratory.[3]

3. Information compromised in the Data Breach represents a gold mine for data thieves and includes personally identifying information ("PII") and protected health information ("PHI") such as names, medical information, clinical test information and dates of service, and Social Security numbers (collectively, "PII" and "PHI" is "Private Information").

4. Plaintiffs bring this class action lawsuit individually and on behalf of those similarly situated to address Defendants' inadequate safeguarding of Plaintiffs' and Class Members' Private Information that Defendants collected and maintained.

5. Defendants maintained the Private Information collected from Plaintiffs and Class Members in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendants' computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure

[1] Enzo Biochem, Inc. SEC Filing (May 30, 2023), https://www.sec.gov/Archives/edgar/data/316253/000121390023044007/ea178836-8k_enzobiohem.htm

[2] Enzo Biochem, Inc., About Us, https://www.enzo.com/corporate/about-us (last accessed June 25, 2023); Enzo Biochem, Inc., Home Page, https://www.enzoclinicallabs.com/ (last accessed June 25, 2023).

[3] *Id*.

Private Information from those risks left that Private Information in a vulnerable condition. In addition, Enzo Defendants and their employees failed to properly monitor the computer network and IT systems that housed the Private Information.

6. Enzo Defendants failed to timely detect and report the Data Breach, and to timely notify affected consumers, including Plaintiffs and Class Members, which made Plaintiffs and Class Members vulnerable to identity theft without any warnings that they needed to act to prevent unauthorized use of their Private Information.

7. In failing to adequately protect Plaintiffs' and the Class Members' Private Information, failing to adequately notify them about the Data Breach, and by obfuscating the nature of the Data Breach, Defendants violated state and federal law and harmed millions of their consumers.

8. Plaintiffs and Class Members are victims of Defendants' negligence and inadequate cybersecurity measures. Specifically, Plaintiffs and Class Members trusted Defendants with their Private Information, but Defendants betrayed that trust, including by failing to properly use up-to-date security practices and measures to prevent the Data Breach, and the exfiltration and theft of Plaintiffs' and Class Members' sensitive Private Information.

9. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names, and giving false information to police during an arrest.

10. As a result of the Data Breach, Plaintiffs and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiffs and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

11. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

12. Indeed, Defendants, themselves, encourage Class Members to spend time responding to the Data Breach. In announcing the Data Breach, Defendants have encouraged Class Members to review correspondence and contact Defendants separately if they do not get the notice of the Data Breach, instructing Class Members to call them on a dedicated line.[4] When Class Members do receive formal notice, Defendants instruct them to carry out a number of tasks, including reviewing their financial and credit card statements.

13. Accordingly, Plaintiffs bring this action against Defendants seeking redress for their unlawful conduct and asserting claims for: (i) negligence; (ii) breach of contract; (iii) unjust enrichment; (iv) breach of fiduciary duty; (v) breach of confidence; (vi) invasion of privacy; (vii) bailment, and (viii) declaratory and injunctive relief, as well as various state statutory claims.

[4] Notice of Data Security Incident, https://www.enzoclinicallabs.com/Uploaded/Website-Notice.pdf (last accessed June 25, 2023).

Through these claims, Plaintiffs seek damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

THE PARTIES

A. Plaintiffs

1. Plaintiff Elyssa Crimeni

14. Plaintiff Elyssa Crimeni ("Plaintiff Crimeni") is an adult individual and citizen of New York.

15. Enzo collected and stored Plaintiff Crimeni's PHI and PII as a condition of providing Plaintiff with medical lab work.

16. Plaintiff Crimeni received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

17. Plaintiff Crimeni values her privacy and makes every effort to keep her personal information private.

18. Since the Data Breach, Plaintiff Crimeni has been the victim of identity theft.

19. On or about June 8, 2023, Plaintiff Crimeni received an alert from Chase Bank about an unauthorized inquiry made on her bank account that she did not recognize.

20. Further, on or about October 2023, Experian, a consumer credit reporting agency, notified Plaintiff Crimeni that her confidential information was detected on the 'dark web'.

21. Since the Data Breach, Plaintiff Crimeni has experienced a significant increase in the frequency of spam messages and phone calls from individuals who have clearly obtained her private information.

22. Plaintiff Crimeni faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff more effectively.

23. As a result of the Data Breach, Plaintiff Crimeni has had to spend more than 40 hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

24. Plaintiff Crimeni is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Crimeni to embarrassment and depriving her of any right to privacy whatsoever.

25. As a result of Defendants' conduct, Plaintiff Crimeni has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

26. Plaintiff Crimeni will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

2. Plaintiff Elizabeth Delgrosso

27. Plaintiff Elizabeth Delgrosso ("Plaintiff Delgrosso") is an adult individual and citizen of New Jersey.

28. Plaintiff Delgrosso's PHI and PII was stored and handled by Enzo.

29. Plaintiff Delgrosso has used Enzo facilities to obtain medical lab work.

30. Plaintiff Delgrosso received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

31. Plaintiff Delgrosso values her privacy and makes every effort to keep her personal information private.

32. Since the Data Breach, Plaintiff Delgrosso has been the victim of identity theft.

33. On or about October 13, 2023, Wells Fargo, a bank, notified Plaintiff Delgrosso via email that her credit score dropped, and that a credit card was opened in her name on or about July 2023. Charges on that July 2023 credit card were over $1,000.00.

34. Upon information and belief, Plaintiff Delgrosso has received alerts from consumer credit monitoring companies that her information may have been exposed to the 'dark web'.

35. Since the Data Breach, Plaintiff Delgrosso has experienced a significant increase in the frequency of spam messages and telephone calls from individuals who have clearly obtained her private information.

36. Plaintiff Delgrosso faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Delgrosso more effectively.

37. As a result of the Data Breach, Plaintiff Delgrosso has had to spend over 10 hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

38. Plaintiff Delgrosso is now forced to live with the anxiety that her PHI and PII may be disclosed to the entire world, thereby subjecting Plaintiff to embarrassment and depriving her of any right to privacy whatsoever.

39. As a result of Defendants' conduct, Plaintiff has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

40. Plaintiff Delgrosso remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Delgrosso faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

41. Plaintiff Delgrosso will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

3. Plaintiff Annette DiIorio

42. Plaintiff Annette DiIorio ("Plaintiff DiIorio") is an adult individual and citizen of the State of New York.

43. In the course of receiving medical treatment, Plaintiff DiIorio's PHI and PII was collected and stored by Enzo.

44. Plaintiff DiIorio received a letter from Enzo notifying her that she is a victim of the Data Breach and has suffered the unauthorized exposure of her PHI and PII.

45. Plaintiff DiIorio values her privacy and makes every effort to keep her personal information private.

46. Since the Data Breach, Plaintiff DiIorio has been the victim of identity theft.

47. Plaintiff DiIorio has experienced a significant increase in the frequency of spam phone calls and messages from individuals who have obtained her private information.

48. Plaintiff DiIorio also received a notification from a consumer credit reporting agency that her information has been detected on the 'dark web'.

49. Plaintiff DiIorio faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff DiIorio more effectively.

50. As a result of the Data Breach, Plaintiff DiIorio has had to spend over 15 hours of her time researching the Data Breach and monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

51. Plaintiff DiIorio is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff DiIorio to embarrassment and depriving her of any right to privacy whatsoever.

52. As a result of Defendants' conduct, Plaintiff DiIorio has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

53. Plaintiff DiIorio remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff DiIorio faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

54. Plaintiff DiIorio will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

4. Plaintiff Eliana Epstein

55. Plaintiff Elianna Epstein ("Plaintiff Epstein") is an adult individual and citizen of Massachusetts.

56. Plaintiff Epstein's PHI and PII was stored and handled by Enzo.

57. Since approximately 2020, Plaintiff Epstein has used Enzo facilities to obtain medical lab work.

58. Plaintiff Epstein received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

59. Plaintiff Epstein values her privacy and makes every effort to keep her personal information private.

60. Since the Data Breach, Plaintiff Epstein has been the victim of identity theft.

61. After the Data Breach, Creditwise, a consumer credit reporting service from CapitalOne, a credit card company, notified Plaintiff Epstein that her confidential information was exposed on the 'dark web'.

62. Since the Data Breach, Plaintiff Epstein has experienced a significant increase in the frequency of spam telephone calls and emails from individuals who have clearly obtained her private information.

63. Plaintiff Epstein faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Epstein more effectively.

64. As a result of the Data Breach, Plaintiff Epstein has had to spend about 12 hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

65. Plaintiff Epstein is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Epstein to embarrassment and depriving her of any right to privacy whatsoever.

66. As a result of Defendants' conduct, Plaintiff Epstein has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

67. Plaintiff Epstein remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Epstein faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

68. Plaintiff Epstein will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

5. Plaintiff Elizabeth Garfield

69. Plaintiff Elizabeth Garfield ("Plaintiff Garfield") is an adult individual and citizen of New York.

70. Enzo collected and stored Plaintiff Garfield's PII and PHI.

71. Since approximately 2018, Plaintiff Garfield has used Enzo facilities to obtain medical lab work.

72. Plaintiff Garfield received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

73. Plaintiff Garfield values her privacy and makes every effort to keep her personal information private.

74. Since the Data Breach, Plaintiff Garfield has experienced a significant increase in the frequency of spam telephone calls and emails from individuals who have clearly obtained her private information.

75. On about September 22, 2023, Plaintiff Garfield received a phone call from an individual claiming to be a representative of TD Bank and alerting Plaintiff to a $142.00 charge. After significant investigation, Plaintiff Garfield found out that the caller who had clearly obtained her PII was an impersonator that the charge was not real.

76. Plaintiff Garfield faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Garfield more effectively.

77. As a result of the Data Breach, Plaintiff Garfield has had to spend over 9 hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

78. Plaintiff Garfield is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Garfield to embarrassment and depriving her of any right to privacy whatsoever.

79. As a result of Defendants' conduct, Plaintiff Garfield has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

80. Plaintiff Garfield remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Garfield faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

81. Plaintiff Garfield will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

6. Plaintiff Gita Garfinkel

82. Plaintiff Gita Garfinkel ("Plaintiff Garfinkel") is an adult individual and citizen of New York.

83. Plaintiff Garfinkel's PHI and PII was stored and handled by Enzo.

84. Plaintiff Garfinkel received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

85. Plaintiff Garfinkel values her privacy and makes every effort to keep her personal information private.

86. Since the Data Breach, Plaintiff Garfinkel has experienced a significant increase in the frequency of spam telephone calls and emails from individuals who have clearly obtained her

private information.

87. Plaintiff Garfinkel faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Garfinkel more effectively.

88. As a result of the Data Breach, Plaintiff Garfinkel has had to spend several hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

89. Plaintiff Garfinkel is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Garfinkel to embarrassment and depriving her of any right to privacy whatsoever.

90. As a result of Defendants' conduct, Plaintiff Garfinkel has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

91. Plaintiff Garfinkel remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Garfinkel faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

92. Plaintiff Garfinkel will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

7. Plaintiff Mark Guthart

93. Plaintiff Mark Guthart ("Plaintiff Guthart") is an adult individual and citizen of New York.

94. Plaintiff Guthart's PHI and PII was stored and handled by Enzo.

95. Before the Data Breach, Plaintiff Guthart has used Enzo facilities to obtain medical lab work.

96. Plaintiff Guthart received a letter from Enzo notifying him of the Data Breach and of the unauthorized exposure of his PHI and PII.

97. Plaintiff Guthart values his privacy and makes every effort to keep his personal information private.

98. Since the Data Breach, Plaintiff Guthart has experienced a significant increase in the frequency of spam messages and telephone calls from individuals who have clearly obtained his private information.

99. After the Data Breach, Plaintiff Guthart has experienced an increase in calls and/or texts relating to medical appointments with unfamiliar doctors.

100. Plaintiff Guthart faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on his PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Guthart more effectively.

101. As a result of the Data Breach, Plaintiff Guthart has had to spend about 40 hours monitoring his accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

102. Plaintiff Guthart is now forced to live with the anxiety that his PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting

Plaintiff Guthart to embarrassment and depriving him of any right to privacy whatsoever.

103. As a result of Defendants' conduct, Plaintiff Guthart has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of his private and confidential personal information, the loss of the benefit of his contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

104. Plaintiff Guthart remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Guthart faces a substantial risk of out-of-pocket fraud losses, such as loans opened in his name, medical services billed in his name, tax return fraud, utility bills opened in his name, credit card fraud, and similar identity theft.

105. Plaintiff Guthart will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

8. Plaintiff Tony Johnson

106. Plaintiff Tony Johnson ("Plaintiff Johnson") is an adult individual and citizen of Connecticut.

107. Plaintiff Johnson's PHI and PII was stored and handled by Enzo.

108. Since approximately 2020, Plaintiff Johnson has used Enzo facilities to obtain medical lab work.

109. Plaintiff Johnson received a letter from Enzo notifying him of the Data Breach and of the unauthorized exposure of his PHI and PII.

110. Plaintiff Johnson values his privacy and makes every effort to keep his personal information private.

111. Since the Data Breach, Plaintiff Johnson has been the victim of identity theft.

112. Since the Data Breach, Plaintiff Johnson has experienced a significant increase in the frequency of spam telephone calls and emails.

113. Plaintiff Johnson faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on his PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Johnson more effectively.

114. As a result of the Data Breach, Plaintiff Johnson has had to spend several hours monitoring his accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

115. As a result of Defendants' conduct, Plaintiff Johnson has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of his private and confidential personal information, the loss of the benefit of his contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

116. Plaintiff Johnson remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Johnson faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in his name, tax return fraud, utility bills opened in his name, credit card fraud, and similar identity theft – particularly since the compromised information may include Social Security numbers.

9. Plaintiff Nino Khakhiasvili

117. Plaintiff Nino Khakhiasvili ("Plaintiff Khakhiasvili") is an adult individual and citizen of Florida.

118. Plaintiff Khakhiasvili's PHI and PII was stored and handled by Enzo.

119. Since approximately 2021, Plaintiff Khakhiasvili has used Enzo facilities to obtain medical lab work.

120. Plaintiff Khakhiasvili received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

121. Plaintiff Khakhiasvili values her privacy and makes every effort to keep her personal information private.

122. Since the Data Breach, Plaintiff Khakhiasvili has been the victim of identity theft. On October 12, 2023, Plaintiff Khakhiasvili received a notification from Chase Bank that Chase detected a fraudulent charge of $44.48 on her bank account. Chase Bank notified Plaintiff Khakhiasvili that it would be closing out the card and issuing her another card.

123. Since the Data Breach, Plaintiff Khakhiasvili has experienced a significant increase in the frequency of spam telephone calls and emails from individuals who have clearly obtained her private information.

124. Since approximately April 2023, Plaintiff Khakhiasvili has received spam calls and/or messages about every hour. Plaintiff receives about two spam messages per week, and about five email messages per day on her personal email account. About 70% of the spam phone calls come from purported financial institutions offering pre-approval for credit or loans.

125. Plaintiff Khakhiasvili faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters

will use exposed information to target Plaintiff Khakhiasvili more effectively.

126. As a result of the Data Breach, Plaintiff Khakhiasvili has had to spend about 5 hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

127. Plaintiff Khakhiasvili is now forced to live with the anxiety that her PHI and PII may be disclosed to the entire world, thereby subjecting Plaintiff Khakhiasvili to embarrassment and depriving her of any right to privacy whatsoever.

128. As a result of Defendants' conduct, Plaintiff Khakhiasvili has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

129. Plaintiff Khakhiasvili remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Khakhiasvili faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

130. Plaintiff Khakhiasvili will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

10. Plaintiff Margo Kupinska

131. Plaintiff Margo Kupinska ("Plaintiff Kupinska") is an adult individual and citizen of New York.

132. Before the Data Breach, Plaintiff Kupinska had used Enzo facilities to obtain medical lab work. In doing so, Plaintiff Kupinska provided Enzo with her PII and PHI.

133. Plaintiff Kupinska received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

134. Plaintiff Kupinska values her privacy and makes every effort to keep her personal information private.

135. Since the Data Breach, Plaintiff Kupinska has been the victim of identity theft.

136. In or about June 2023, Plaintiff Kupinska noticed a fraudulent charge of approximately $110.00 on her Bank of America card that she did not authorize. Plaintiff Kupinska spent roughly one hour calling her bank two different times in order to get this fraudulent charge remedied.

137. Since the Data Breach, Plaintiff Kupinska has experienced a significant increase in the frequency of spam messages and telephone calls from individuals who have clearly obtained her private information.

138. Plaintiff Kupinska faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff more effectively.

139. As a result of the Data Breach, Plaintiff Kupinska has had to spend about 20 hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

140. Plaintiff Kupinska is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Kupinska to embarrassment and depriving her of any right to privacy whatsoever.

141. As a result of Defendants' conduct, Plaintiff Kupinska has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

142. Plaintiff Kupinska remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Kupinska faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft – particularly since the compromised information may include Social Security numbers.

11. Plaintiff Paula Magnani

143. Plaintiff Paula Magnani ("Plaintiff Magnani") is an adult individual and citizen of New Jersey.

144. Before the Data Breach, Plaintiff Magnani had used Enzo facilities to obtain medical lab work. In doing so, Plaintiff Magnani provided Enzo with her PII and PHI.

145. Plaintiff Magnani received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII dated May 31, 2023.

146. Plaintiff Magnani values her privacy and makes every effort to keep her personal information private.

147. Since the Data Breach, Plaintiff Magnani has experienced a significant increase in the frequency of medical-related spam emails suggesting these individuals have clearly obtained her private information in connection with this Data Breach.

148. Plaintiff Magnani faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff more effectively.

149. Plaintiff Magnani is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Magnani to embarrassment and depriving her of any right to privacy whatsoever.

150. As a result of Defendants' conduct, Plaintiff Magnani has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

151. Plaintiff Magnani remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Magnani faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft – particularly since the compromised information may include Social Security numbers.

12. Plaintiff Shana McHugh

152. Plaintiff Shana McHugh ("Plaintiff McHugh") is an adult individual and citizen of Connecticut.

153. Plaintiff McHugh's PHI and PII was stored and handled by Enzo.

154. Upon information and belief, Plaintiff McHugh used Enzo in the course of obtaining medical care.

155. Plaintiff McHugh received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

156. Plaintiff McHugh values her privacy and makes every effort to keep her personal information private.

157. Since the Data Breach, Plaintiff McHugh has experienced a significant increase in the frequency of spam telephone calls in Arabic from individuals who have clearly obtained her private information.

158. Plaintiff McHugh faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff McHugh more effectively.

159. As a result of the Data Breach, Plaintiff McHugh has had to spend about three hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

160. Plaintiff McHugh is now forced to live with the anxiety that her PHI and PII, may be disclosed to the entire world, thereby subjecting Plaintiff McHugh to embarrassment and depriving her of any right to privacy whatsoever.

161. As a result of Defendants' conduct, Plaintiff McHugh has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the

loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

162. Plaintiff McHugh remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff McHugh faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

163. Plaintiff McHugh will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

13. Plaintiff Mary Namorato

164. Plaintiff Mary Namorato ("Plaintiff Namorato") is an adult individual and citizen of New York.

165. Plaintiff Namorato's PHI and PII was stored and handled by Enzo.

166. Since approximately 2018, Plaintiff Namorato has used Enzo facilities to obtain medical lab work.

167. Plaintiff Namorato received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

168. Plaintiff Namorato values her privacy and makes every effort to keep her personal information private.

169. Since the Data Breach, Plaintiff Namorato has been the victim of identity theft.

170. On about July 28, 2023 and September 26, 2023, Experian, a consumer credit reporting company, notified Plaintiff that it found her PII on the 'dark web'.

171. Since the Data Breach, Plaintiff Namorato has experienced a significant increase in the frequency of spam telephone calls and text messages from individuals who have clearly obtained her private information.

172. Plaintiff Namorato faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Namorato more effectively.

173. As a result of the Data Breach, Plaintiff Namorato has had to spend several hours a month monitoring her accounts to detect suspicious and fraudulent activity and deleting spam to mitigate against potential harm.

174. Plaintiff Namorato is now forced to live with the anxiety that her PHI and PII may be disclosed to the entire world, thereby subjecting Plaintiff Namorato to embarrassment and depriving her of any right to privacy whatsoever.

175. As a result of Defendants' conduct, Plaintiff Namorato has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

176. Plaintiff Namorato remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Namorato faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

177. Plaintiff Namorato will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

14. Plaintiff Robert Pastore

178. Plaintiff Robert Pastore ("Plaintiff Pastore") is an adult individual and citizen of California.

179. Plaintiff Pastore's PHI and PII was stored and handled by Enzo.

180. Over three decades ago, Plaintiff Pastore used an Enzo facility in the course of obtaining medical care.

181. Plaintiff Pastore received a letter from Enzo notifying him of the Data Breach and of the unauthorized exposure of his PHI and PII.

182. Plaintiff Pastore values his privacy and makes every effort to keep his personal information private.

183. Since the Data Breach, Plaintiff Pastore has been the victim of identity theft.

184. On about October 30, 2023, Brand Yourself, an online reputation management company, notified Plaintiff Pastore that his name appeared on the 'dark web'.

185. On about November 2, 2023, Experian, a consumer credit reporting company, notified Plaintiff Pastore that his name appeared 16 times on the dark web.

186. Since the Data Breach, Plaintiff Pastore has experienced a significant increase in the frequency of spam telephone calls and/or messages from individuals who have clearly obtained his private information.

187. During approximately the past 30 days before November 2, 2023, there has been an increase in spam phone calls to Plaintiff Pastore using his private information.

188. Plaintiff Pastore faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on his PHI and PII, as potential fraudsters will use exposed information to target Plaintiff more effectively.

189. As a result of the Data Breach, Plaintiff Pastore has had to spend time about 38 hours monitoring his accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

190. Plaintiff Pastore is now forced to live with the anxiety that his PHI and PII may be disclosed to the entire world, thereby subjecting Plaintiff Pastore to embarrassment and depriving him of any right to privacy whatsoever.

191. As a result of Defendants' conduct, Plaintiff Pastore has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of his private and confidential personal information, the loss of the benefit of his contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

192. Plaintiff Pastore remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Pastore faces a substantial risk of out-of-pocket fraud losses, such as loans opened in his name, medical services billed in his name, tax return fraud, utility bills opened in his name, credit card fraud, and similar identity theft.

193. Plaintiff Pastore will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

15. Plaintiff Saribel Rodriguez

194. Plaintiff Saribel Rodriguez ("Plaintiff Rodriguez") is an adult individual and citizen of New York.

195. Plaintiff Rodriguez's PHI and PII was stored and handled by Enzo.

196. Since approximately 2023, Plaintiff Rodriguez has used Enzo facilities to obtain medical lab work.

197. Plaintiff Rodriguez received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

198. Plaintiff Rodriguez values her privacy and makes every effort to keep her personal information private.

199. Since the Data Breach, Plaintiff Rodriguez has experienced a significant increase in the frequency of spam messages and telephone calls from individuals who have clearly obtained her private information.

200. Plaintiff Rodriguez faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Rodriguez more effectively.

201. Since the Data Breach, Plaintiff Rodriguez has received bills for medical services which she has already paid in full.

202. As a result of the Data Breach, Plaintiff Rodriguez has had to spend about 5 hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

203. Plaintiff Rodriguez is now forced to live with the anxiety that her PHI and PII may be disclosed to the entire world, thereby subjecting Plaintiff Rodriguez to embarrassment and

depriving her of any right to privacy whatsoever.

204. As a result of Defendants' conduct, Plaintiff Rodriguez has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

205. Plaintiff Rodriguez remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Rodriguez faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

206. Plaintiff Rodriguez will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

16. Plaintiff Izza Shah

207. Plaintiff Izza Shah ("Plaintiff Shah") is an adult individual and citizen of New York.

208. Since approximately 2023, Plaintiff Shah has used Enzo facilities to obtain medical lab work. In the course of obtaining medical lab work from Enzo, Plaintiff Shah provided Enzo with her PII and PHI.

209. Plaintiff Shah received a letter from Enzo notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

210. Plaintiff Shah values her privacy and makes every effort to keep her personal information private.

211. Since the Data Breach, Plaintiff Shah has experienced a significant increase in the frequency of spam telephone calls and emails from individuals who have clearly obtained her private information.

212. During the past few months, Plaintiff Shah has experienced an increase in suspicious phone calls, texts, and emails.

213. Plaintiff Shah faces a substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff Shah more effectively.

214. As a result of the Data Breach, Plaintiff Shah has had to spend over six hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

215. Plaintiff Shah is now forced to live with the anxiety that her PHI and PII may be disclosed to the entire world, thereby subjecting Plaintiff Shah to embarrassment and depriving her of any right to privacy whatsoever.

216. As a result of Defendants' conduct, Plaintiff Shah has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, out of pocket expenses, emotional distress, and other economic and non-economic harm.

217. Plaintiff Shah remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff Shah faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

218. Plaintiff Shah will now be forced to expend additional time to freeze credit, to review credit reports and monitor financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

B. Defendants

219. Defendant Enzo Biochem is a corporation incorporated in New York, with its headquarters in Farmingdale, New York. Enzo Biochem's principal place of business is 81 Executive Blvd., Suite 3, Farmingdale, New York 11735. Defendant is a citizen of the State of New York.

220. Defendant Enzo Clinical is a wholly owned subsidiary of Defendant Enzo Biochem, incorporated in New York, with its principal place of business located at 60 Executive Blvd., Farmingdale, New York 11735.

JURISDICTION AND VENUE

221. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because some Plaintiffs and at least one member of the putative Class, as defined below, are citizens of a different state than Defendants Enzo Biochem and Enzo Clinical; there are more than 100 putative class members; and, the amount in controversy exceeds $5 million exclusive of interest and costs.

222. This Court has general personal jurisdiction over Defendants because Defendants maintain their principal places of business in Farmingdale, New York, regularly conduct business

in New York, and have sufficient minimum contacts in New York.

223. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' principal places of business are in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

DEFENDANTS' BUSINESS

224. Founded in 1976, Enzo Biochem is a life sciences company which "lead[s] the convergence of clinical laboratories, life sciences, and intellectual property through the development of unique diagnostic platform technologies that provide numerous advantages over previous standards." [5] Enzo Biochem conducts all business activities through three wholly owned subsidiaries, including Enzo Clinical.[6]

225. Enzo Clinical, is a wholly-owned subsidiary of Enzo Biochem which operates a full-service clinical reference laboratory and the "GoTestMeNow" Online Platform.[7] Enzo Clinical markets itself as "one of the leading regional labs in the country, as we combine the extensive testing capabilities of a large laboratory with the convenience and personalized service of a local one." [8]

226. Enzo Defendants generate approximately $100 million annual revenue.[9] Enzo trades on the New York Stock Exchange under the stock symbol ENZ. [10]

---

[5] Enzo Clinical Labs, Inc., https://www.enzo.com/ (last accessed June 25, 2023).
[6] *Id.*
[7] Enzo Clinical Labs, Inc., https://www.enzoclinicallabs.com/ (last accessed June 25, 2023).
[8] *Id.*
[9] *Enzo Biochem Reports Fourth Quarter and Fiscal Year 2022 Financial Results and Provides Business Update*, GlobalNewswire (Oct. 14, 2022) https://www.globenewswire.com/en/news-release/2022/10/14/2534560/0/en/Enzo-Biochem-Reports-Fourth-Quarter-and-Fiscal-Year-2022-Financial-Results-and-Provides-Business-Update.html.
[10] Yahoo! Finance, *Enzo Biochem, Inc. (ENZ)*, https://finance.yahoo.com/quote/ENZ/ (last accessed June 23, 2023).

227. To obtain healthcare and related clinical laboratory services, patients, like Plaintiffs and Class Members, must provide their doctors, medical professionals, or Defendants directly with highly sensitive Private Information. As part of their business, Defendants then compile, store, and maintain the Private Information they receive from patients and healthcare professionals who utilize Defendants' services. In their over 45 years of experience, Defendants have served millions of individuals, indicating that they have created and maintain a massive repository of Private Information: a particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

228. On information and belief, in the ordinary course of their business of providing medical care and services, Enzo maintains the Private Information of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial and/or payment information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Health insurance information;
- Clinical testing information and results;
- Other information that Defendants may deem necessary to provide services and care.

229. Additionally, Defendants may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends, and/or family members.

230. Because of the highly sensitive and personal nature of the information Defendants acquire and store with respect to patients and other individuals, Enzo, upon information and belief, promises to, among other things: keep PHI private; comply with health care industry standards related to data security and Private Information, including HIPAA; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

231. As HIPAA covered business entities (*see infra*), Enzo Defendants are required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

232. However, Enzo Defendants did not maintain adequate security to protect their systems from infiltration by cybercriminals, and they waited nearly two months to publicly disclose the Data Breach.

233. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

THE DATA BREACH AND NOTICE LETTER

234. According to the Notice Letter Enzo provided to Plaintiffs and Class Members, Enzo was subject to a ransomware attack where unauthorized parties accessed Private Information on Enzo's networks between April 4-6, 2023.[11]

235. On April 6, 2023, Enzo Defendants were alerted to unusual activity on their network. In response, according to the Notice Letter, Enzo "began an investigation with the assistance of a cybersecurity firm" and "took steps to secure our systems."[12]

236. Through Enzo's investigation, Enzo determined that "an unauthorized party accessed files on our systems" and that the files contained certain Private Information, including things like patients' name, date of service, and clinical test information.[13] According to Enzo's SEC disclosure, the Data Breach additionally compromised the Social Security numbers of approximately 600,000 affected individuals. Enzo asserts that it believes no financial information was taken but the experiences of many Plaintiffs contradict this claim and, upon information and belief, Plaintiffs allege that such information was likely accessed.

237. The breach notice does not state who this "unauthorized party" was, or whether a ransomware demand was made to or paid by Enzo.

238. Enzo waited nearly two months from the date it learned of the Data Breach and the highly sensitive nature of the Private Information impacted to publicly disclose the Data Breach and notify affected individuals.

[11] *See* Notification of Data Security Incident to Plaintiff Paula Magnani, Ex. A. ("Notice Letter).
[12] See *id.*
[13] *See id.*

239. In the aftermath of the Data Breach, Enzo Defendants reportedly intend to "continue to take steps to enhance the security of our computer systems and the data we maintain."[14] In other words, Defendants admit additional security was required, but there is no indication whether these steps are adequate to protect Plaintiffs' and Class Members' Private Information going forward.

240. In the Notice Letter Defendants recommended that Plaintiffs and Class Members "review statements you receive from your healthcare providers for accuracy and contact your providers with any questions," but offers no credit monitoring or identity theft services to the majority of the nearly 2.5 million affected individuals.[15] Although Enzo is reportedly "offering complimentary credit monitoring and identity theft protection services to those whose Social Security numbers were involved," Enzo has given no details such as indication of the duration and extent of the services it is offering.[16]

241. According to Enzo, Plaintiffs' and Class Members' Private Information was exfiltrated and stolen in the attack.

242. Enzo's accessed systems contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

243. As HIPAA covered business entities (*see infra*) that collect, create, and maintain significant volumes of Private Information, the targeted attack was a foreseeable risk which Enzo

[14] *See* Notice Letter.
[15] *See 2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack*, DARKReading (June 5, 2023), https://www.darkreading.com/attacks-breaches/2-5m-impacted-by-enzo-biochem-data-leak-after-ransomware-attack. *See also* Notice Letter.
[16] Notice of Data Security Incident, https://www.enzoclinicallabs.com/Uploaded/Website-Notice.pdf (last accessed June 25, 2023).

Defendants were aware of and which Enzo Defendants knew they had a duty to guard against. This is particularly true because the targeted attack was a ransomware attack.[17] It is well-known that healthcare businesses such as Defendants', which collect and store the confidential and sensitive PII/PHI of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

244. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiffs and Class Members.

245. Defendants had obligations created by HIPAA, contract, industry standards, common law, and their own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

246. Plaintiffs and Class Members provided their Private Information to Enzo, either directly or indirectly, with the reasonable expectation and mutual understanding that Enzo Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

247. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Enzo assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiffs' and Class Members' Private

[17] *See 2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack*, DARKReading (June 5, 2023), https://www.darkreading.com/attacks-breaches/2-5m-impacted-by-enzo-biochem-data-leak-after-ransomware-attack.

Information from unauthorized disclosure.

248. Due to Enzo's inadequate security measures and Enzo's delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

Enzo Defendants are Covered Entities Subject to HIPAA

249. Defendants had duties to ensure that all information they collected and stored was secure, and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiffs' and Class Members' Private Information.

250. Enzo Defendants are HIPAA covered entities that provide services to patients and/or healthcare and medical service providers. As a regular and necessary part of their businesses, Defendants collect the highly sensitive Private Information of their and their clients' patients.

251. Enzo Biochem's most recent Form 10-K filed with the Securities and Exchange Commission states that its:

> Covered Entities and Business Associates are subject to potentially significant civil and criminal penalties for violating HIPAA. Under the Omnibus Rule, health care providers, such as laboratories, that are subject to HIPAA as a Covered Entity are also vicariously liable for violations of HIPAA based on acts or omissions of their agents, including Business Associates, when the agent is acting within the scope of the agency....We may also be subject to state laws that are not pre-empted by HIPAA to the extent the state law is more stringent than HIPAA, provides individuals with greater rights with respect to their protected health information, or are broader in scope than HIPAA.[18]

252. As covered entities under HIPAA, Defendants are required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that they acquire,

[18] https://www.sec.gov/Archives/edgar/data/316253/000121390022064086/f10k2022_enzobio.htm

receive, and collect, and Defendants are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

Defendants' Conduct Violates HIPAA Obligations to Safeguard Private Information

253. Because Enzo Defendants are covered by HIPAA (see 45 C.F.R. § 160.102) they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

254. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[19] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

255. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

256. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

257. HIPAA requires that Defendants implement appropriate safeguards for this information.

[19] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

258. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

259. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

260. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires HIPAA covered entities and their business associates, like Defendants, to provide notification following a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e. non-encrypted data—to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[20]

261. HIPAA requires covered entities to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. §

[20] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/forprofessionals/breach-notification/index.html (emphasis added).

164.530(e).

262. HIPAA requires covered entities to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

263. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." See US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." See US Department of Health & Human Services, Guidance on Risk Analysis.[21]

264. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported." The four-factor risk assessment focuses on:

[21] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

(1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[22]

265. Despite these requirements, Defendants failed to comply with their duties under HIPAA and their own Privacy Practices. Indeed, Defendants failed to:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiffs' and Class Members' Private Information;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h) Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i) Conduct the Four Factor Risk Analysis following the Breach;

[22] 78 Fed. Reg. 5641-46; see also 45 C.F.R. § 164.304.

j) Properly send notice to Plaintiffs and Class Members pursuant to 45 C.F.R. §§ 164.400-414;

k) Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

l) Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

266. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

267. Defendants failed to comply with their duties under HIPAA and their own privacy policies despite being aware of the risks associated with unauthorized access of Plaintiffs' and Class Members' Private Information.

268. Enzo Defendants' Data Breach resulted from a combination of insufficiencies that indicate that Enzo Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards.

Enzo Defendants had Legal and Equitable Duties to Safeguard Plaintiffs' and Class Members Private Information

269. Due to the nature of Defendants' businesses, which include providing a range of clinical medical services for patients and services for Defendants' healthcare and medical clients, including storing and maintaining electronic health records, Enzo Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information

that they know and understand to be sensitive and confidential.

270. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Enzo Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

271. Plaintiffs and Class Members are or were patients, or are the executors or surviving spouses of patients, whose medical records and Private Information were maintained by, or who received health-related or other services from Enzo and directly or indirectly entrusted Enzo with their Private Information.

272. Plaintiffs and Class Members relied on Enzo to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiffs and Class Members reasonably expected that Enzo would safeguard their highly sensitive information and keep that Private Information confidential.

273. As described throughout this Complaint, Enzo did not reasonably protect, secure, or store Plaintiffs' and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Enzo maintained. Consequently, cybercriminals circumvented Enzo's security measures, resulting in a significant data breach.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice

274. As HIPAA covered entities handling medical patient data, Enzo's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

275. At all relevant times, Enzo knew, or should have known that Plaintiffs' and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Enzo failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks that Enzo should have anticipated and guarded against.

276. In light of high-profile data breaches at other health care providers, Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

277. These data breaches have been a consistent problem for the past several years, providing Defendants sufficient time and notice to harden their systems and engage in better, more comprehensive cybersecurity practices.

278. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[23]

[23] *2022 Breach Barometer*, PROTENUS, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (last visited May. 7, 2023).

279. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[24]

280. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

281. Indeed, cyberattacks against the healthcare industry have been common for over eleven years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cybercriminals will no doubt lead to an escalation in cybercrime."[25]

[24] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited May. 7, 2023).
[25] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

282. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[26] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[27] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[28]

283. Cyberattacks on medical systems, like Defendants', have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive.. . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[29]

284. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [30]

---

[26] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited May. 7, 2023).
[27] *Id.*
[28] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.
[29] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[30] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022),

285. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[31] In this case, Enzo stored the records of *millions* of patients.

286. Private Information, like that stolen from Enzo, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[32]

287. Indeed, cybercriminals are also monetizing encrypted data by saving it until decryption methods are developed, at which point the data will be combined with the rest of the "fullz." This practice is well-known among entities actively monitoring for such risks, as Defendants should reasonably have been doing.

288. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

289. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[33]

---

https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[31] See *id.*
[32] See *id*.
[33] *See* Maria Henriquez*, Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

290. Enzo was on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[34]

291. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[35]

292. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

293. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014

[34] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited May 7, 2023).
[35] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[36]

294. As HIPAA covered entities, Enzo Defendants should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

Defendants Fail to Comply with FTC Guidelines

295. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

296. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[37] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[38]

---

[36] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.
[37] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[38] *Id*.

297. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

298. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

299. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

300. Defendants failed to properly implement basic data security practices.

301. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

302. Defendants were at all times fully aware of their obligation to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Fail to Comply with Industry Standards

303. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

304. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendants, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limitations on which employees can access sensitive data.

305. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

306. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

307. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and, ultimately, causing the Data Breach.

308. As discussed above, Defendants are covered entities under HIPAA.

309. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

310. Enzo is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

311. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

312. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

313. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

314. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

315. The Data Breach resulted from a combination of insufficiencies that demonstrate Enzo failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

316. Cyberattacks and data breaches at health care companies like Defendants' are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

317. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[39]

318. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with a deterioration in timeliness and patient outcomes, generally.[40]

319. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[41]

---

[39] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[40] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[41] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

320. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate the pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

321. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[42]

322. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

[42] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 7, 2023).

323. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

324. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[43]

325. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

326. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

327. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[43] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

328. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

329. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

330. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for many years to come.

331. Private Information can sell for as much as $363 per record according to the Infosec Institute.[44] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

332. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[45] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for

[44] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[45] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.

unemployment benefits, or apply for a job using a false identity.[46] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

333. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

334. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[47]

335. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[48]

336. Medical information is especially valuable to identity thieves.

337. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

[46] *Id*.
[47] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[48] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[49]

338. Drug manufacturers, medical device manufacturers, clinical laboratories, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

339. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

340. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

341. Defendants placed themselves in a position where they owed a duty to Plaintiffs and Class Members by virtue of the sensitivity of the data that they collected. Indeed, because of Defendants, Plaintiffs and Class Members were placed in a worse position than they would have been had Defendants not collected and maintained their data. Defendants knew the risk that they created and, accordingly, were in the best position to protect Plaintiffs and Class Members by virtue of the special relationship that they created with them.

[49] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Apr. 6, 2023).

DEFENDANTS' DATA BREACH

342. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

343. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Enzo's computer network and systems for multiple days which contained unsecured and unencrypted Private Information.

344. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants.

Plaintiffs' and Class Members' Damages

345. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiffs and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Yet, to date, Defendants have not even offered to provide the majority of victims of the Data Breach with limited subscriptions to fraud and identity monitoring services. Defendants have done nothing to compensate Plaintiffs or Class Members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiffs and Class Members as a result of the Data Breach.

346. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

347. Plaintiffs' and Class Members' names, clinical test information, dates of service, and Social Security numbers, and financial information were all likely compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendants' computer system(s).[50]

348. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

349. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes

[50] *See 2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack*, DARKReading (June 5, 2023), https://www.darkreading.com/attacks-breaches/2-5m-impacted-by-enzo-biochem-data-leak-after-ransomware-attack.

changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

350. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

351. As a direct and proximate result of Defendants' conduct, Plaintiffs' and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

352. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

353. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

354. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiffs' and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

355. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

356. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

357. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendants and/or Defendants' healthcare partners was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

358. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

359. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

360. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected

from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

361. Further, as a result of Defendants' conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

362. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiffs' Experiences

363. Plaintiffs provided their Private Information Enzo either directly or via their healthcare providers as part of the process of obtaining medical services provided by Enzo Defendants, and Plaintiffs trusted that this information would be safeguarded according to state and federal law.

364. Upon information and belief, Plaintiffs were each presented with standard forms to complete prior to receiving medical services that required their PII and PHI. Upon information and belief, Defendants received and maintain the information Plaintiffs were required to provide to their doctors or medical professionals or to Enzo directly.

365. Plaintiffs are very careful with their Private Information. They store any documents containing their Private Information in a safe and secure location or destroys the documents. Plaintiffs have never knowingly transmitted unencrypted sensitive Private Information over the

internet or any other unsecured source. Moreover, Plaintiffs diligently choose unique usernames and passwords for their various online accounts.

366. As a result of the Data Breach, Plaintiffs each made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring their credit.

367. Plaintiffs were each forced to spend multiple hours attempting to mitigate the effects of the Data Breach. They will continue to spend valuable time they otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

368. Plaintiffs suffered actual injury and damages from having thier Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information, a form of intangible property that Enzo obtained from Plaintiffs and/or Plaintiffs' doctors and medical professionals; (b) violation of their privacy rights; (c) the theft of their Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) failure to receive the benefit of their bargains; and (g) nominal and statutory damages.

369. Plaintiffs have also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of their Private Information, which they believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using their Private Information for purposes of identity theft and fraud. Plaintiffs have also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her Social Security number, medical records, and clinical test

results.

370. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiffs will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

371. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

372. Plaintiffs bring this action against Enzo individually and on behalf of all other persons similarly situated ("the Class").

373. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Nationwide Class").**

374. Plaintiffs also propose to represent state subclasses, ("State Subclasses" and collectively with the Class, the "Classes") defined as follows and subject to amendment as appropriate:

> **New Jersey State Subclass:** All New Jersey residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "New Jersey Subclass").
>
> **New York State Subclass:** All New York residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who

were sent a notice of the Data Breach (the "New York Subclass").

Connecticut State Subclass: All Connecticut residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Connecticut Subclass").

California State Subclass: All California residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "California Subclass").

Florida State Subclass: All Florida residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Florida Subclass").

Massachusetts State Subclass: All Massachusetts residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Massachusetts Subclass").

375. Excluded from the Classes are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

376. Plaintiffs reserve the right to amend or modify the Class definitions or create additional subclasses as this case progresses.

377. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. Defendants disclosed to the SEC that the Private Information of approximately 2,470,000 Class Members was compromised in Data Breach.

378. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common

questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breached implied contracts with Plaintiffs and Class Members;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

379. Typicality. Named Plaintiffs' claims are typical of those of other Class Members because named Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

380. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

381. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the data of Plaintiffs and Class Members was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

382. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for

Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

383. Defendants have acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

384. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;
b. Whether Defendants owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;
c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and
f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

385. Finally, all members of the proposed Classes are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

386. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein.

387. By collecting and storing the Private Information of Plaintiffs and Class Members, in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

388. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

389. Plaintiffs and Class Members are a well-defined, foreseeable, and probable group of patients that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

390. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

391. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

392. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. .. practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

393. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

394. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

395. Plaintiffs and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

396. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

397. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

398. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

399. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

400. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

401. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

402. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

403. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein.

404. In addition to the common law and special relationship duties alleged herein, Defendants also owed a duty to safeguard Plaintiffs' and Class Members' Private Information by statute.

405. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by

laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

406. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

407. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. .. practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

408. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

409. Defendants breached that duty, which, as discussed herein, caused Plaintiffs and Class Members injuries, for which they are entitled to damages.

410. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injuries and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT III
Gross Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

411. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein.

412. Defendants knew that they were protecting the most sensitive Private Information about Plaintiffs and Class Members that exists—healthcare information—which can impact anything from housing, employment, benefits, education, and other areas of an individual's life.

413. When that Private Information is compromised, the effects can be devastating to individuals, such that Defendants knew or should have known about these effects and the need to keep this information secure and protected.

414. Defendants' failure to keep this information safe was grossly negligent, as Defendants were aware of the grave consequences of not keeping this information secure.

415. As a result of Defendants' gross negligence, Plaintiffs and Class Members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT IV
Breach of Contract
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

416. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein.

417. Defendants entered into various contracts with its clients, including healthcare providers, to provide software services to its clients.

418. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that

Defendants agreed to collect and protect through their services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class were the direct and primary objective of the contracting parties.

419. Defendants knew that if they were to breach these contracts with their healthcare provider clients, the clients' consumers, including Plaintiffs and the Class, would be harmed by, among other things, fraudulent misuse of their Private Information.

420. Defendants breached their contracts with their clients when they failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' Private Information.

421. As a reasonably foreseeable result of the breach, Plaintiffs and the Class were harmed by Defendants failure to use reasonable data security measures to store their Private Information, including but not limited to, the actual harm through the loss of their Private Information to cybercriminals.

422. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
Breach of Contracts to Which Plaintiffs and Class Members are Intended Third-Party Beneficiaries
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

423. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein. This claim is pleaded in the alternative to the breach of implied contract and breach of contract claims (Count IV and Count VI).

424. Defendants had valid contracts with certain physicians for the purpose of providing clinical testing and test results on behalf of patients. A principal purpose of those contracts was to

securely store, transmit and safeguard the PII and PHI of Plaintiffs and Class Members.

425. Upon information and belief, Defendants and each of the contracting healthcare providers expressed an intention that Plaintiffs and Class Members were intended third party beneficiaries of these agreements.

426. Plaintiffs and Class Members are also intended third-party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Defendants intended to give the beneficiaries the benefit of the promised performance.

427. Defendants breached its agreements with the contracting healthcare providers by allowing the Data Breach to occur, and as otherwise set forth herein.

428. Defendants' breach caused foreseeable and material damages to Plaintiffs and Class Members.

COUNT VI
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

429. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein.

430. Defendants acquired and maintained the Private Information of Plaintiffs and the Class that it received either directly or from its healthcare provider customers.

431. When Plaintiffs and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, and clinical laboratories, including Defendants.

432. Plaintiffs and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

433. Plaintiffs and the Class were required to deliver their Private Information to Defendants as part of the process of obtaining services provided by Defendants. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

434. Enzo Defendants solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants, or, alternatively, provided Plaintiffs' and Class Members' information to doctors or other healthcare professionals, who then provided to Defendants.

435. Defendants accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services or Plaintiffs and Class Members.

436. In accepting such information and payment for services, Defendants entered into an implied contract with Plaintiffs and the other Class Members whereby Defendants became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

437. Alternatively, Plaintiffs and Class Members were the intended beneficiaries of data protection agreements entered into between Defendants and healthcare providers.

438. In delivering their Private Information to Defendants and paying for healthcare services, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard the data as part of that service.

439. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

440. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

441. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

442. Had Defendants disclosed to Plaintiffs and Class (or their physicians) that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Private Information to Defendants (or their physicians to provide to Defendants).

443. Defendants recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

444. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Defendants.

445. Defendants breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

446. As a direct and proximate result of Defendants' conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT VII
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

447. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein.

448. This count is pleaded in the alternative to all breach of contract claims, above (Counts IV-VI).

449. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from money they make based upon protecting Plaintiffs' and Class Members' Private Information.

450. There is a direct nexus between money paid to Defendants and the requirement that Defendants keep Plaintiffs' and Class Members' Private Information confidential and protected.

451. Plaintiffs and Class Members paid Defendants and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendants.

452. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

453. Protecting data from Plaintiffs and the rest of the Class Members is integral to Defendants' business. Without their data, Defendants would be unable to provide the clinical lab

testing services comprising Defendants' core business.

454. Plaintiffs' and Class Members' data has monetary value, and Defendants realize this benefit when they choose to store such data.

455. Plaintiffs and Class Members directly and indirectly conferred a monetary benefit on Defendants. They indirectly conferred a monetary benefit on Defendants by purchasing goods and/or services from entities that contracted with Defendants, and from which Defendants received compensation to protect certain data. Plaintiffs and Class Members directly conferred a monetary benefit on Defendants by supplying Private Information, which has value, from which value Defendants derive their business value, and which should have been protected with adequate data security.

456. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

457. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

458. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by

industry standards.

459. Defendants acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

460. If Plaintiffs and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants (or to their physician to provide to Defendants).

461. Plaintiffs and Class Members have no adequate remedy at law.

462. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) loss or privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

463. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

464. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

COUNT VIII
Bailment
(*On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses*)

465. Plaintiffs re-allege and incorporates by reference paragraphs 1–371 as if set fully forth herein.

466. Plaintiffs and Class Members provided Private Information to Defendants—either directly or through healthcare providers and their business associates—which Defendants were under a duty to keep private and confidential.

467. Plaintiffs' and Class Members' Private Information is personal property, and it was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

468. Plaintiffs' and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendants were aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

469. Once Defendants accepted Plaintiffs' and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiffs nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

470. Defendants did not safeguard Plaintiffs' or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

471. Defendants' failure to safeguard Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

472. As a result of Defendants' failure to keep Plaintiffs' and Class Members' Private Information secure, Plaintiffs and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—is appropriate.

COUNT IX
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

473. Plaintiffs re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

474. In light of the special relationship between Defendants and Plaintiffs and Class Members, Defendants became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants do store.

475. Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship with their patients, in particular, to keep secure their Private Information.

476. Defendants breached their fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class

Members' Private Information.

477. Defendants breached their fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

478. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendants' services they received.

479. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT X
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

480. Plaintiffs re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

481. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendants and ultimately accessed and acquired in the Data Breach.

482. At all times during its possession and control of Plaintiffs; and Class Members' Private Information, Defendants were fully aware of the confidential, novel, and sensitive nature of Plaintiffs' and Class Members' Private Information provided to it.

483. As alleged herein and above, Defendants' possession and control of Plaintiffs' and Class Members' highly sensitive Private Information was governed by the expectations of Plaintiffs and Class Members that their Private Information would be collected, stored, and protected in confidence, and that it would not be disclosed to unauthorized third parties.

484. Plaintiffs and Class Members provided their respective Private Information with the understanding that it would be protected and not disseminated to any unauthorized parties.

485. Plaintiffs and Class Members also provided their respective Private Information with the understanding that precautions would be taken to protect it from unauthorized disclosure, and that these precautions would at least include basic principles of information security practices.

486. Defendants voluntarily received, in confidence, Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

487. Due to Defendants' failure to prevent, detect, and/or avoid the Data Breach from occurring by, inter alia, failing to follow best information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized criminal third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

488. But for Defendants' unauthorized disclosure of Plaintiffs' and Class Members' Private Information, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third-party criminals. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as the resulting damages.

489. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendants knew or should have known that its security systems were insufficient to protect the Private Information that is coveted and misused by thieves worldwide. Defendants also failed to observe industry standard information security practices.

490. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered damages as alleged herein.

COUNT XI
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

491. Plaintiffs re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

492. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendants, as alleged above.

493. The contracts respecting which Plaintiffs and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that

Defendants would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiffs' PII and PHI from unauthorized disclosure and to comply with state laws and regulations.

494. A "special relationship" exists between Defendants and the Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members who sought medical services from Enzo Clinical and, in doing so, entrusted Defendants, pursuant to their requirements and Privacy Notice, with their PII and PHI.

495. Despite this special relationship with Plaintiffs, Defendants did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' PII and PHI.

496. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendants.

497. Defendants' failure to act in good faith in complying with the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations.

498. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendants' breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT XII
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Subclasses)

499. Plaintiffs re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

500. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendants mishandled.

501. As a result of Defendants' conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

502. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

503. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

504. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

505. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

506. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT XIII
Violation of the New York Deceptive Trade Practices Act
New York General Business Law ("GBL") § 349
(On Behalf of Plaintiffs Crimeni, DiIorio, Garfield, Garfinkel, Guthart, Kupinska, Namorato, Rodriguez, and Shah and the New York Subclass)

507. Plaintiffs Crimeni, DiIorio, Garfield, Garfinkel, Guthart, Kupinska, Namorato, Rodriguez, and Shah ("New York Plaintiffs") re-allege and incorporates by reference paragraphs 1–371 as if fully set forth herein.

508. New York Deceptive Trade Practices Act, N.Y. Gen. Bus. Law § 349, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

509. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the N.Y. Gen. Bus. Law § 349. The conduct alleged herein is a "business practice" within the meaning of the N.Y. Gen. Bus. Law § 349, and the deception occurred within New York State.

510. Defendants stored New York Plaintiffs' and New York Subclass Members' Private Information in Defendants' electronic databases. Defendants knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept New York Plaintiffs' and New York Subclass Members' Private Information secure and prevented the loss or misuse of that Private Information. Defendants did not disclose to New York Plaintiffs and New York Subclass Members that its data

systems were not secure.

511. New York Plaintiffs and New York Subclass Members would not have provided their Private Information if they had been told or knew that Defendants failed to maintain sufficient security thereof, and its inability to safely store New York Plaintiffs' and New York Subclass Members' Private Information.

512. As alleged herein in this Complaint, Defendants engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of N.Y. Gen. Bus. Law § 349, including but not limited to:

- Representing that their services were of a particular standard or quality that it knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect New York Plaintiffs' and New York Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' and New York Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that they would protect the privacy and confidentiality of New York Plaintiffs' and New York Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure New York Plaintiffs' and New York Subclass Members' Private Information; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' and New York Subclass Members' Private

Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

513. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

514. Such acts by Defendants are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendants. These deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, N.Y. Gen. Bus. Law § 349. 207. In addition, Defendants' failure to secure patients' Private Information violated the FTCA and therefore violates N.Y. Gen. Bus. Law § 349.

515. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of New York Plaintiffs and New York Subclass Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely. New York Plaintiffs and New York Subclass Members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

516. The aforesaid conduct violated N.Y. Gen. Bus. Law § 349, in that it is a restraint on trade or commerce.

517. Defendants' violations of N.Y. Gen. Bus. Law § 349 have an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have had their Private Information stored on Defendants' electronic database, many of whom have been

impacted by the Data Breach.

518. As a direct and proximate result of these deceptive trade practices, New York Plaintiffs and New York Subclass Members are entitled to judgment under N.Y. Gen. Bus. Law § 349, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

519. On information and belief, Defendants formulated and conceived of the systems used to compile and maintain patient information largely within the state of New York, oversaw its data privacy program complained of herein from New York, and its communications and other efforts to hold participant data largely emanated from New York.

520. Most, if not all, of the alleged misrepresentations and omissions by Defendants that led to inadequate measures to protect patient information occurred within or were approved within New York.

521. Defendants' implied and express representations that it would adequately safeguard New York Plaintiffs' and New York Subclass Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of N.Y. Gen. Bus. Law § 349.

522. Accordingly, New York Plaintiffs, on behalf of themselves and New York Subclass Members, bring this action under N.Y. Gen. Bus. Law § 349 to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT XIV
New York Constitution Right to Privacy
(On Behalf of Plaintiffs Crimeni, DiIorio, Garfield, Garfinkel, Guthart, Kupinska, Namorato, Rodriguez, and Shah and the New York Subclass)

523. Plaintiffs Crimeni, DiIorio, Garfield, Garfinkel, Guthart, Kupinska, Namorato, Rodriguez, and Shah ("New York Plaintiffs") re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

524. The New York Constitution provides: "[n]o person shall be deprived of life, liberty or property without due process of law." (N.Y. Const., art. I, § 6.)

525. New York Plaintiffs and the New York Subclass had a legally recognized and protected privacy interest in the personal medical information provided to and obtained by Defendants, including but not limited to an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes.

526. New York Plaintiffs and the New York Subclass reasonably expected Defendants would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their personal medical information.

527. Defendants' conduct described herein resulted in a serious invasion of the privacy of New York Plaintiffs and the New York Subclass, as the release of personal medical information, including but not limited to names, social security numbers, dates of medical lab testing, and medical lab test results could highly offend a reasonable individual.

528. As a direct consequence of the actions as identified above, New York Plaintiffs and the New York Subclass suffered harms and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time

dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed.

COUNT XV
Violation of the New Jersey Consumer Fraud Act
N.J.S.A. § 56:8-1, *et seq*.
(On Behalf of Plaintiffs Delgrosso and Magnani and the New Jersey Subclass)

529. Plaintiffs Delgrosso and Magnani ("New Jersey Plaintiffs") re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

530. New Jersey Plaintiffs and all New Jersey Subclass members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1

531. Defendants are a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

532. Defendants' conduct as alleged related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

533. Defendants advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of New Jersey.

534. Defendants solicited New Jersey Plaintiffs and New Jersey Subclass Members to do business and uniformly and knowingly misrepresented that by joining, their Private Information was safe, confidential, and protected from intrusion, hacking, or theft.

535. Defendants misrepresented that they would protect the privacy and confidentiality of New Jersey Plaintiffs' and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable security measures.

536. Defendants intended to mislead New Jersey Plaintiffs and New Jersey Subclass Members and induce them to rely on their misrepresentations and omissions.

537. Defendants failed to implement and maintain reasonable security and privacy measures to protect New Jersey Plaintiffs' and New Jersey Subclass Members' Private Information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

538. Defendants failed to provide notice to New Jersey Plaintiffs and New Jersey Subclass Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

539. Defendants' acts and omissions, as set forth evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2. 261. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, New Jersey Plaintiffs and New Jersey Subclass Members are required to expend sums to protect and recover their Private Information, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, and thereby suffered ascertainable economic loss.

540. New Jersey Plaintiffs and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT XVI
Violation of the Connecticut Unfair Trade Practices Act ("CUTPA")
Conn. Gen. Stat. §§ 42-110a, *et seq*.
(On Behalf of Plaintiffs Johnson and McHugh and the Connecticut Subclass)

541. Plaintiffs Johnson and McHugh ("Connecticut Plaintiffs"), re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

542. Defendants are each a "person" as defined by Conn. Gen. Stat. § 42-110a(3).

543. Defendants engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Conn. Gen. Stat. § 42-110b(a).

544. Defendants' representations and omissions include both implicit and explicit representations.

545. Defendants' unfair and deceptive acts and practices include:

- Failing to implement and maintain reasonable security and privacy measures to protect Connecticut Plaintiffs' and the Connecticut Subclass' PII, which was a direct and proximate cause of the Data Breach;

- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

- Failing to comply with common law and statutory duties pertaining to the security and privacy of Connecticut Plaintiffs' and the Connecticut Subclass' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Connecticut security breach law, Conn. Gen. Stat. § 36a-701b;

- Misrepresenting that they would protect the privacy and confidentiality of Connecticut Plaintiffs' and the Connecticut Subclass' PII, including by implementing and maintaining reasonable security measures;

- Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Connecticut Plaintiffs' and the Connecticut Subclass' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Connecticut security breach law, Conn. Gen. Stat. § 36a701b;

- Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Connecticut Plaintiffs' and the Connecticut Subclass' PII; and

- Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Connecticut Plaintiffs' and the Connecticut Subclass' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Connecticut Security Breach law, Conn. Gen. Stat. § 36a-701b. 221.

546. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

547. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Connecticut Plaintiffs and the Connecticut Subclass, that their PII was not exposed and misled Connecticut Plaintiffs and the Connecticut Subclass into believing they did not need to take actions to secure their identities.

548. The injury to consumers from Defendants' conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PII or the security of their identity or credit.

549. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of injury which consumers could not have reasonably avoided because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security programs, Defendants created an asymmetry of information between themselves and consumers that precluded consumers from taking action to avoid or mitigate injury.

550. Defendants' inadequate data security had no countervailing benefit to consumers or to competition

551. Defendants also engaged in "deceptive" acts and practices in violation of Conn. Gen. Stat. § 42-110b(a), including:

- Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

- Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

- Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

552. Defendants intended to mislead Connecticut Plaintiffs and the Connecticut Subclass and induce them to rely on their misrepresentations and omissions.

553. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

554. Had Defendants disclosed to Connecticut Plaintiffs and the Connecticut Subclass that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants were trusted with sensitive and valuable PII regarding tens of thousands of consumers, including Connecticut Plaintiffs and the Connecticut Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of their security controls, and the security controls of their agents and representatives, secret from the public. Accordingly, because Defendants held themselves out as

maintaining a secure platform for PII data, Connecticut Plaintiffs and the Connecticut Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

555. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII in their possession. This duty arose because Defendants were trusted with sensitive and valuable PII regarding tens of thousands of consumers, including Connecticut Plaintiffs and the Connecticut Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls, and the security controls of their agents and representatives, a secret from the public. Accordingly, because Defendants held themselves out as maintaining a secure platform for PII data, Connecticut Plaintiffs, the Class, and the Connecticut Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Connecticut Plaintiffs and the Connecticut Subclass—and Defendants, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants.

556. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security programs, Defendants created an asymmetry of information between them and consumers that precluded consumers from taking action to avoid or mitigate injury.

557. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

558. Defendants also engaged in "deceptive" acts and practices in violation of Conn. Gen. Stat. § 42-110b(a), including:

- Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

- Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

- Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

559. Defendants intended to mislead Connecticut Plaintiffs and the Connecticut Subclass and induce them to rely on their misrepresentations and omissions.

560. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

561. Had Defendants disclosed to Connecticut Plaintiffs and the Connecticut Subclass that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants were trusted with sensitive and valuable PII regarding tens of thousands of consumers, including Connecticut Plaintiffs and the Connecticut Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of their security controls, and the security controls of their agents and

representatives, secret from the public. Accordingly, because Defendants held themselves out as maintaining a secure platform for PII data, Connecticut Plaintiffs and the Connecticut Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

562. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII in their possession. This duty arose because Defendants were trusted with sensitive and valuable PII regarding tens of thousands of consumers, including Connecticut Plaintiffs and the Connecticut Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls, and the security controls of their agents and representatives, a secret from the public. Accordingly, because Defendants held themselves out as maintaining a secure platform for PII data, Connecticut Plaintiffs and the Connecticut Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers— including Connecticut Plaintiffs and the Connecticut Subclass—and Defendants, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants.

563. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Connecticut Plaintiffs and the Connecticut Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

564. Defendants' violations present a continuing risk to Connecticut Plaintiffs and the Connecticut Subclass as well as to the general public.

565. Connecticut Plaintiffs and the Connecticut Subclass seek all monetary and non-monetary relief allowed by law under Conn. Gen. Stat. § 42-110g(a), including actual damages; punitive damages; injunctive relief; restitution; reasonable attorneys' fees and costs; and any other relief that the Court deems appropriate.

COUNT XVII
Violation of the California Consumer Privacy Act
(Cal. Civ. Code § 1798.150 ("CCPA"))
(On Behalf of Plaintiff Pastore and the California Subclass)

566. Plaintiff Pastore re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

567. At all relevant times, Defendants were "businesses" under the terms of the CCPA as sole proprietorships, partnerships, limited liability companies, corporations, associations, or other legal entities operating in the State of California that collect consumers' personal information, and that have annual operating revenue above $25 million.

568. At all relevant times, Plaintiff Pastore and the California Subclass were "consumers" under the terms of the CCPA as natural persons as defined in Section 17014 of Title 18 of the California Code of Regulations.

569. By the acts described above, Defendants violated the CCPA by negligently and recklessly collecting, maintaining, and controlling their customers' sensitive personal medical information and by designing, maintaining, and controlling systems that exposed their customers' sensitive personal medical information of which Defendants had control and possession to the risk of exposure to unauthorized persons, thereby violating their duty to implement and maintain

reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. Defendants allowed unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and nonredacted personal information of Plaintiffs and other customers, including their personal medical information.

570. Plaintiff Pastore has complied with the requirements of California Civil Code section 1798.150(b)1 and attach herewith as Exhibit 1 a true and correct copy of the letter of June 20, 2023,[51] providing Defendants with written notice of the specific provisions of the CCPA [California] Plaintiffs allege have been violated via certified mail.

571. As a result of Defendants' violations, Plaintiff Pastore and the California Subclass are entitled to all actual and compensatory damages according to proof or statutory damages allowable under the CCPA, whichever are higher, and to such other and further relief as this Court may deem just and proper.

COUNT XVIII
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.82 ("CRA")
(On Behalf of Plaintiff Pastore and the California Subclass)

572. Plaintiff Pastore re-alleges and incorporate by reference paragraphs 1–371 as if fully set forth herein.

573. At all relevant times, Defendants were "businesses" under the terms of the CRA as corporations or other groups operating in the State of California that owned or licensed computerized data that included the personal information of Plaintiff Pastore and the California Subclass.

[51] *See* Ex. B.

574. At all relevant times, Plaintiff Pastore and the California Subclass were "customers" under the terms of the CRA as natural persons who provided personal information to Defendants for the purpose of purchasing or leasing a product or obtaining a service from Defendants.

575. By the acts described above, Defendants violated the CRA by allowing unauthorized access to customers' personal medical information and then failing to inform them when the unauthorized use occurred for weeks or months, and in the case of Plaintiff Pastore, for 58 days, thereby failing in their duty to inform their customers of unauthorized access expeditiously and without delay

576. As a direct consequence of the actions as identified above, Plaintiff Pastore and the California Subclass incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed, and related losses and injuries that they would not have otherwise incurred had Defendants immediately informed them of the unauthorized use.

577. As a result of Defendants' violations, Plaintiff Pastore and the Class are entitled to all actual and compensatory damages according to proof, to non-economic injunctive relief allowable under the CRA, and to such other and further relief as this Court may deem just and proper.

COUNT XIX
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, et seq. ("CMIA")
(On Behalf of Plaintiff Pastore and the California Subclass)

578. Plaintiff Pastore re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

579. At all relevant times, Defendants subject to the CMIA as Defendants were "providers of health care" under the terms of the CMIA. Defendants were businesses organized to maintain and make available medical information for the diagnosis and treatment of medical patients; businesses offering software, including mobile applications, designed to maintain medical information in order to make information available to patients or providers of health care for purposes of diagnosis, treatment, or management of a medical condition; persons or entities engaged in the art and science of medicine and to such other arts and sciences as may be included within the field of medicine; persons or entities engaged in clinical laboratory practice and sciences; and persons or entities that operated organized outpatient health facilities providing direct medical services or diagnostic services to patients. Alternatively, Defendants were subject to the CMIA as Defendants were "contractors" under the terms of the CMIA as persons or entities providing contract services to providers of health care or that were part of a medical service group or organization.

580. At all relevant times, Plaintiff Pastore and the California Subclass were "patients" under the terms of the CMIA natural persons who received health care services from a provider of health care and to whom medical information pertains.

581. Defendants were in possession of Plaintiff Pastore and the California Subclass's "medical information," as defined by the CMIA, including individually identifiable information

derived from providers of health care or contractors regarding Plaintiff Pastore and the California Subclass's medical history, physical condition, or treatment.

582. Defendants violated the CMIA by disclosing medical information regarding Plaintiff Pastore and the California Subclass without first obtaining authorization; by negligently maintaining the confidential medical information of Plaintiff Pastore and the California Subclass; by creating, maintaining, preserving, or storing the medical information of Plaintiff Pastore and the California Subclass in a manner that failed to preserve the confidentiality of the information; and by creating, maintaining, or operating an electronic health record system or electronic medical record system that failed to protect and preserve the integrity of electronic medical information of Plaintiff Pastore and the California Subclass.

583. Defendants' negligence allowed the medical information of Plaintiff Pastore and the California Subclass to be accessed by unauthorized third persons and permitted it to escape or spread from its normal place of storage, and therefore negligently released the information within the meaning of CMIA, at which time the medical information was viewed by unauthorized persons.

584. As a result of Defendants' violations, Plaintiff Pastore and the California Subclass are entitled to all actual and compensatory damages according to proof or statutory damages allowable under the CMIA, whichever are higher, to punitive damages, to attorneys' fees and costs of litigation, and to such other and further relief as this Court may deem just and proper.

COUNT XX
California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, et seq. ("CLRA")
(On Behalf of Plaintiff Pastore and the California Subclass)

585. Plaintiff Pastore re-alleges and incorporate by reference paragraphs 1–371 as if fully set forth herein.

586. At all relevant times, Plaintiff Pastore and the California Subclass were "consumers" as under the terms of the CLRA as individuals seeking or acquiring, by purchase or lease, goods or services for personal, family, or household purposes.

587. At all relevant times, Defendants' actions and conduct constituted transactions for the sale or lease of goods or services to consumers under the terms of the CLRA. The clinical lab work offered and sold by Defendants constitute "services" under the CLRA.

588. By the acts described above, Defendants violated California Civil Code section 1770(a)(5), by the use of untrue or misleading statements and omissions and representing that goods and services had characteristics or benefits they do not have.

589. By the acts described above, Defendants violated California Civil Code section 1770(a)(14), by representing that Enzo maintained the highest level of data security and a promise to personal medical safeguard information from unauthorized use when Defendants knew such rights were not conferred.

590. Defendants knew, or should have known, that their representations and advertisements about the nature of their data security and promise to fully reimburse funds lost due to unauthorized use were false or misleading and were likely to deceive a reasonable consumer. No reasonable consumer would use Defendants' products or engage Defendants' services if they knew Defendants were not taking reasonable measures to safeguard their personal

medical information or if they knew Defendants would not make good on their promise to fully reimburse funds lost due to unauthorized use.

591. Plaintiff Pastore have complied with the requirements of California Civil Code section 1782 and attaches herewith as Exhibit 2 a true and correct copy of his letter of June 20, 2023[52] providing Defendants with written notice of the specific provisions of the CLRA Plaintiffs allege have been violated via certified mail.[53]

592. Pursuant to California Civil Code section 1780(d), attached hereto as Exhibit 3 is a declaration on behalf of Plaintiff Pastore showing that this action has been commenced in the proper forum.[54]

593. Defendants generated revenue by way of Plaintiff Pastore and the California Subclass paying or providing access to medical insurance payments when entering transactions with Defendants where Defendants were the direct beneficiaries of these payments. Defendants' services were of lesser quality and value than Defendants represented in that Defendants did not take reasonable measures to safeguard customers' personal medical information. In reliance on Defendants' misrepresentations about its products and services, Plaintiff Pastore and the California Subclass entered transactions with Defendants that they would not have, or for which Plaintiff Pastore and the California Subclass would have paid less but for Defendants' representations.

---

[52] *Id*.

[53] Pursuant to Civil Code section 1782(d), Plaintiffs presently seek only injunctive relief under the CLRA and, upon the expiration of time prescribed by Civil Code section 1782, will amend this complaint to confirm the Defendants have declined or failed to correct, repair, replace, or otherwise rectify their violation and to add claims for actual, punitive, and statutory damages, as appropriate.

[54] *Supra.*

594. As a direct and proximate consequence of the actions as identified above, Plaintiff Pastore and the California Subclass suffered injury in fact, harms, and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed.

595. Defendants' conduct described herein was malicious, fraudulent, and wanton in that Defendants intentionally and knowingly provided misleading information to Plaintiffs and the Class and refused to remedy the breach of their system long after learning of the inadequacy of their data protection measures and the unauthorized use of customers' accounts.

596. As a result of Defendants' violations, Plaintiff Pastore and the California Subclass seek a court order enjoining the above-described wrongful acts and practices of Defendants and for restitution and disgorgement. Plaintiffs also seek public injunctive relief as provided for under California Civil Code section 1750, in addition to reasonable attorneys' fees and costs pursuant to California Civil Code section 1780(e), and such other and further relief as this Court may deem just and proper.

COUNT XXI
California Constitution Right to Privacy
Cal. Const., art I, § 1
(On Behalf of Plaintiff Pastore and the California Subclass)

597. Plaintiff Pastore re-alleges and incorporate by reference paragraphs 1–371 as if fully set forth herein.

598. The California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." (Cal. Const., art. I, § 1.)

599. Plaintiff Pastore and the California Subclass had a legally recognized and protected privacy interest in the personal medical information provided to and obtained by Defendants, including but not limited to an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes such as the theft of funds and property.

600. Plaintiff Pastore and the California Subclass reasonably expected Defendants would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their personal medical information and the unauthorized use of their accounts.

601. Defendants' conduct described herein resulted in a serious invasion of the privacy of Plaintiff Pastore and the California Subclass, as the release of personal medical information, including but not limited to names, social security numbers, dates of lab testing service, and lab testing results could highly offend a reasonable individual.

602. As a direct consequence of the actions as identified above, Plaintiff Pastore and the California Subclass suffered harms and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed

COUNT XXII
California Unfair Competition Act
Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL")
(On Behalf of Plaintiff Pastore and the California Subclass)

603. Plaintiff Pastore re-alleges and incorporate by reference paragraphs 1–371 as if fully set forth herein.

604. By engaging in the above-described unfair business acts and practices, Defendants committed and continue to commit one or more acts of unlawful and unfair conduct within the meaning of the UCL. These acts and practices constitute a continuing and ongoing unlawful business activity defined by the UCL, and justify the issuance of an injunction, restitution, and other equitable relief pursuant to the UCL.

605. Defendants' acts and practices constitute a continuing and ongoing unlawful business activity defined by the UCL. Defendants failed and continue to fail to implement and maintain reasonable security procedures and practices appropriate to protect the personal information; failed and continue to fail to inform their customers of unauthorized access expeditiously and without delay; and made and continue to make misrepresentations to customers regarding the nature and quality of their data protection, all in violation of, inter alia, the following California laws:

a. California Civil Code section 1798.150(a);

b. California Civil Code section 1798.82(a);

c. California Civil Code section 56.36;

d. California Civil Code section 56.101;

e. California Civil Code section 1770(a)(5);

f. California Civil Code section 1770(a)(14); and,

g. California Constitution, article I, section 1.

606. Defendants' acts and practices constitute a continuing and ongoing unfair business activity defined by the UCL. Defendants' conduct is contrary to the public welfare as it transgresses civil statutes designed to protect individuals' constitutional and statutory right to privacy, violates established public policy, and has been pursued to attain an unjustified monetary advantage for Defendants by creating personal disadvantage and hardship to their customers. As such, Defendants' business practices and acts have been immoral, unethical, oppressive and unscrupulous and has caused injury to customers far greater than any alleged countervailing benefit.

607. Defendants generated revenue by way of Plaintiff Pastore and the California Subclass paying or generating medical insurance payments when entering transactions with Defendants where Defendants were the direct beneficiaries of these payments. Defendants' services were of lesser quality and value than Defendants represented in that Defendants did not take reasonable measures to safeguard customers' personal medical information. In reliance on Defendants' misrepresentations about its products and services, Plaintiff Pastore and the California Subclass entered transactions with Defendants that they would not have, or for which Plaintiff Pastore and the California Subclass would have paid less but for Defendants' representations.

608. As a direct and proximate consequence of the actions as identified above, Plaintiff Pastore and the California Subclass suffered and continue to suffer harms and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated

to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed.

609. Plaintiff Pastore seek an order of this Court awarding restitution and injunctive relief and all other relief allowed under the UCL, including interest and attorneys' fees pursuant to, inter alia, Code of Civil Procedure section 1021.5, and to such other and further relief as this Court may deem just and proper.

COUNT XXIV
Massachusetts Consumer Protection Act
Mass. Gen. Laws Ann. Ch. 93a, §§ 1, *et seq*.
(On Behalf of Plaintiff Epstein and the Massachusetts Sublass)

610. Plaintiff Epstein re-alleges and incorporate by reference paragraphs 1–371 as if fully set forth herein.

611. Plaintiff Epstein brings this claim on behalf of herself and the Florida Subclass against Defendans.

612. This claim is brought individually under the laws of Massachusetts and on behalf of all other natural persons whose Private Information was compromised.

613. Defendants, Plaintiff Epstein and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

614. Defendants operate in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

615. Defendants advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

616. Plaintiff Epstein sent written demands for relief on behalf of herself and Massachusetts Subclass Members pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3)—including, but not limited to on November 10, 2023. Defendants did not respond with a reasonable offer of relief to Massachusetts Subclass Members.

617. Defendants engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including by:

a. Failing to implement and maintain reasonable security and privacy measures to protect Massachusetts Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Massachusetts Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Massachusetts Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Massachusetts Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Failing to timely and adequately notify Massachusetts Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Private Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Massachusetts Subclass Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Massachusetts Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

618. Defendants' acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Defendants solely held the true facts about its inadequate security for Private Information, which Massachusetts Subclass Members could not independently discover.

619. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Massachusetts Subclass Members, that their PII was not exposed and misled Massachusetts Subclass Members into believing they did not need to take actions to secure their identities.

620. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Defendant created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

621. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Massachusetts Subclass Members and induce them to rely on its misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private

Information.

622. Defendants acted intentionally, knowingly, and maliciously to violate Massachusetts' Consumer Protection Act, and recklessly disregarded Massachusetts Subclass Members' rights.

623. As a direct and proximate result of Defendants' unfair and deceptive trade practices, Massachusetts Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

624. Massachusetts Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

COUNT XXIV
Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq*
(On Behalf of Plaintiff Khakhiashvili and the Florida Subclass)

625. Plaintiff Khakhiashvili restates and realleges all preceding allegations in paragraphs 1–371 as if fully set forth herein.

626. Plaintiff Khakhiashvili brings this claim on behalf of himself and the Florida Subclass against Defendants.

627. Plaintiff Khakhiashvili and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

628. Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

629. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Khakhiashvili and Florida Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Khakhiashvili and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of P Plaintiff Khakhiashvili and Florida Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Khakhiashvili and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff Khakhiashvili and Florida Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Khakhiashvili and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

630. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

631. Had Defendants disclosed to Plaintiff Khakhiashvili and Florida Subclass Members that their data systems were not secure and, thus, were vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants were trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff Khakhiashvili and Florida Subclass Members. Defendant accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Khakhiashvili and Florida Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

632. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff Khakhiashvili and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non- monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

633. Plaintiff Khakhiashvili and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

COUNT XXV
Declaratory and Injunctive Relief
(On Behalf of Plaintiffs and the Nationwide Class)

634. Plaintiffs re-allege and incorporate by reference paragraphs 1–371 as if fully set forth herein.

635. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*.

636. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

637. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendants is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

638. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

639. Defendants still possess the Private Information of Plaintiffs and the Class.

640. To Plaintiffs' knowledge, Defendants have made no announcement that it has changed their data storage or security practices relating to the Private Information, beyond the vague claim in the Data Breach Letter that it is "[taking] steps to enhance the security of our

computer systems and the data we maintain."

641. To Plaintiffs' knowledge, Defendants have made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than fifteen years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees, as permitted by law;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Dated: November 13, 2023

Respectfully submitted by,

/s/ James J. Pizzirusso
James J. Pizzirusso
Hausfeld LLP
888 16th St. NW, Suite 300
Washington, DC 20006
T: 202.540.7200
jpizzirusso@hausfeld.com

/s/ Jean S. Martin
Jean S. Martin
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
T: 813.559.4908
jeanmartin@forthepeople.com

Interim Co-Lead Counsel